

REMARKS

This amendment is submitted in response to the Office Action mailed on November 7, 2006. Reconsideration and allowance of this application, as amended, is respectfully requested in view of the remarks that follow.

The three independent claims 1, 17, and 22 are of similar scope – claim 1 is a method claim, while claims 17 and 22 are apparatus claims. Claim 22 differs from claim 17 in that it contains “means for” terminology. These three independent claims will be discussed together in the discussion which follows. Dependant claims having similar scopes will also be discussed together.

Corrections of minor defects have been made to claims 21 and 23. Approval of these corrections is respectfully requested.

A. The Rejection

Independent Claims 1, 17, and 22 and dependent claims 2-16, 18-21, and 23-24 stand rejected under 35 USC §102(e) in view of U.S. Published Application No. US 2004/0181689 A1 which was filed on October 30, 2003 in the United States on behalf of Satoshi Kiyoto, *et al.*

The Examiner may have construed the claims overly broadly by overlooking the fact that many of the words and phrases which appear in the claims are defined in the specification, in a special “Definition of Terms” section that appears in paragraphs [0029] through [0047]. It is applicant’s intention that these definitions be referred to when reading and interpreting the claims. Applicant will refer to these definitions in the discussion which follows. Applicant respectfully requests that the Examiner reconsider the claims construed in the light of these definitions.

B. The Kiyoto, *et al.* Patent Application

The Kiyoto, *et al.* application discloses a VoIP (“Voice over IP” – see par. [0004]) system that facilitates Internet telephony by providing a handshake protocol (shown in Figure

3 of the Kiyoto, *et al.* patent application) whereby two Internet telephony systems can exchange “presence” information and also “security policy” information (Figure 3, steps 501 to 508) before attempting peer-to-peer digitized voice communication across the Internet (Figure 3, steps 509-510). A “user” 9 requests security policy and presence information from a “peer’s communication apparatus” 11-1, and later the “user” 9 registers the security policy information (step 508) and the presence information (step 504) with an intermediate communication apparatus 10.

With reference to Figure 9 of the Kiyoto, *et al.* application, the “presence” information exchanged and registered includes such things as the user’s name (“John”) 919, his or her Internet addresses (“192.168.1.2”) 918, his or her e-mail address (peerA@example.com”) 917, and his or her location (“office”) 920.

With reference to Figure 8 of the Kiyoto, *et al.* application, the “security policy” information exchanged and registered includes: “Source” and “Destination” Internet (810 and 814) and “Port” (812 and 816) addresses (a full Internet address for sending an information packet includes the Internet address of a computer plus a port address on that same computer); whether the TCP protocol 818 (Transmission Control Protocol, a slower protocol that includes error detection and correction) or the UDP protocol 819 (User Datagram Protocol, a faster protocol which does not include error detection and correction) is to be used to convey digitized voice information to and from the specified Internet and port addresses; whether some form of Internet Protocol Security (“ipsec” 825 – see par. [0005]) is to be utilized – and if so, whether some form of authentication (“ah” 826), or encryption (“esp” 827), or compression (“ipcomp” 828), or some combination of these is to be used (see pars. [0061]-[0065]).

In brief summary, the Kiyoto, *et al.* patent application teaches that before beginning to exchange digitized voice packets across the Internet, any two individuals who wish to communicate by means of Internet telephony must each inform the other of the following: Whether the digitized voice message packets are to be UDP datagrams or TCP message packets; to what Internet and Port addresses the message packets are to be sent; whether the message packets are to be encrypted or compressed (and what algorithms are used to perform encryption or compression); and whether authentication is required or not. Clearly, without

exchanging this crucial information, the two individuals will not be able to communicate successfully. If one party is sending out encrypted and compressed message packets, the other party must be made aware of this. By analogy, one using an AM (amplitude modulation) two-way radio tuned to one frequency cannot possibly communicate with another using an FM (frequency modulation) two-way radio tuned to an entirely different frequency. The one must advise the other in some manner that an AM radio tuned to a particular frequency must be used. Likewise, a telephone conversation cannot take place across the Internet between two individuals unless the equipment used by each party to the conversation is adjusted to reflect the other party's Internet and Port addresses, choice of protocol (UDP or TCP), and use or non-use of compression, encryption, and authentication. The Kiyoto, *et al.* patent application teaches one way in which such adjustments can be communicated between the parties so that they may set their Internet telephones accordingly.

C. Independent Claims 1, 17, and 22 Are Not Anticipated By Kiyoto, *et al.*

In contrast to all of the above, the present invention is not a method and system that enables two who wish to communicate across the Internet to learn whether the other is using encryption or compression or authentication or is sending or expecting TCP message packets rather than UDP datagrams as well as to what Internet and port address such datagrams or message packets must be sent. The present invention does not teach anything about such things.

The present invention is a method and system for "auditing the security" of an "enterprise" that includes "plural nodes." (Claim 1, lines 1-2; claim 17, lines 1-2; and claim 22, lines 1-2.) An "enterprise" is defined (by the present application's "Definition of Terms") to be

a collection of computers, software, and networking that interconnects the computing environment of an organization of people. (present application, paragraph [0030])

A "node" is defined to be

a particular device in an enterprise, other than information pathways, to which or from which or through which information may flow over an enterprise network.

Examples of nodes are servers, work stations, other types of computers, printers, routers, switches, and hubs. (present application, paragraph [0031])

A "Security Audit" is defined to be

a formal examination or verification of the security of an enterprise, preferably including (among other things) the configuration of its nodes and other elements, the attitudes of its personnel, and the degree to which physical security policies are actually implemented. (present application, paragraph [0045])

The term "configuration" used in this definition of "Security Audit" is defined to be

any information specific to the static or dynamic configuration of one or more elements or classes of elements residing upon one or more nodes at a given point in time or over a range of time. (present application, paragraph [0034])

And the term "element" used in this definition of the term "configuration" is defined to be

one or more physical devices (CPUs, nodes, computers, hardware, storage systems, etc.) or logical devices (programs or software, firmware, volumes, directories, files, databases, threads, processes, functions, etc.) within an enterprise that can be monitored and/or managed. (present application, paragraph [0033])

When these definitions of terms are taken into account, clearly none of the independent claims 1, 17, and 22 is broad enough to read upon the teachings of the Kiyoto *et al.* patent application. The Kiyoto *et al.* patent application does not teach nor disclose any way of examining or verifying the security of the "nodes" of an "enterprise," and in particular the configuration of the hardware and software "elements" of such "nodes." All the Kiyoto *et al.* patent application teaches is how the computers of two users wishing to communicate can be advised of the level of security that the other computer is employing so that both computers can employ the same level of security and thereby communicate successfully. Kiyoto does not verify the security of the hardware and software elements of the two computers. Kiyoto, instead, blindly accepts either a high level of security or a low level of security and does not judge whether the security is adequate – Kiyoto does not perform a "security audit" as that phrase is defined above and as that phrase is used in the claims now before the Examiner. For this reason, reconsideration and allowance of the claims as presently drafted is respectfully requested.

Method Claim 1 (lines 3 and 4) calls for “collecting” and “analyzing” “security information from the nodes of the enterprise under audit.” Likewise, apparatus Claim 17 (lines 3-6) calls for “collectors associated with nodes” that collect “information concerning the security of the enterprise under audit,” and it further calls for “a security analyzer arranged to analyze the information concerning the security of the enterprise” Claim 22 (lines 3-6) similarly calls for “collector means ...” and “security analyzer means” In the “Definition of Terms,” the term “collectors” is defined to be

a command, or a series of commands, that access, or that cause other programs installed at nodes to access, a node ... to gather configuration information about the node ... and its ... elements and then to return this information to a central site for analysis. (present application, paragraph [0036])

The term “analyzer” is defined to be

a program or rule or other set of instructions defining how configuration information gathered from a node is to be analyzed to develop information for later use in reports and in comparative studies. Analyzers may also identify issues of concern that should be reported to management. ... (present application, paragraph [0041])

The Kiyoto *et al.* patent application does not teach collecting information from the hardware and software elements of a “node” (a computer within an enterprise) and analyzing that collected information to identify issues for later use in comparative security studies or for later use in identifying issues of concern that need to be reported to management. Contrary to this, the only information gathered and conveyed by the Kiyoto *et al.* system is information defining the format of digitized voice information that is to be conveyed across the Internet. This gathered format information is not specifically analyzed for later use in comparative studies or to identify issues of concern to management. This gathered format information is used simply to configure two Internet digitized voice information transceivers so that they become compatible and can then transmit and receive digitized voice information packets properly. For this additional reason, these claims define invention over the Kiyoto, *et al.* patent application.

The final elements of claims 1, 17, and 22 call for the result of the analysis to be compared with “security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group, the result of this comparing step indicating the relative security of the enterprise under audit to that of the peer group of

enterprises.” (Claim 1, lines 5-8. See also Claim 17, lines 7-12 and Claim 22, lines 7-12)
The phrase “peer group” is defined in the “Definition of Terms” section of the present application as follows:

The relevant peer group of an enterprise that is being audited can be defined in several different ways: For example, it can be enterprises assigned to the same business category as the enterprise; enterprises involved in the same (or a similar) industry or business as the enterprise (health, education, military, etc.); enterprises having computers configured similarly to the enterprise’s computers (considering both systems and business configuration); or enterprises required to comply with the same security levels as the enterprise; or a combination of these. (present application, paragraph [0046])

As an example, the Examiner is referred to Figure 6 of the present application, where the security levels of an enterprise named “ACME” in 17 separate security categories are compared to 17 industry average security levels.

For example, and referring to Figure 6, the “PASSWORD” security of ACME’s “nodes” or computers, computed in the manner explained in Figure 3 and the accompanying text, was found to be about “21”. This is below the industry average “PASSWORD” security level, which is “40”. Again in Figure 6, the file “PERMISSIONS” of ACME’s “nodes” or computers, computed in the manner explained in Figure 5 and the accompanying text, was found to be about “85”. This is above the industry average file “PERMISSIONS” security level, which is “80”.

Applicant has carefully studied the Kiyoto *et al.* patent application, but applicant can find nothing whatsoever in any way similar to this claim requirement that the results of a security audit of one enterprise be compared to the combined security audits of a relevant peer group of enterprises.

Accordingly, claims 1, 17, and 22 are believed to define invention over the teachings of the Kiyoto, *et al.* patent application. Their allowance is respectfully requested.

D. The Dependent Claims Are Also In Condition for Allowance

The dependent claims 2-16, 18-21, and 23-24 are also in condition for allowance, since they depend upon the allowable claims 1, 17, or 22. In addition, each dependent claim introduces a feature not to be found in the Kiyoto, *et al.* patent application. The distinguishing features of each dependant claim are summarized briefly below:

Claim 2 requires the peer group information to be derived from “industry standards applicable to the relevant peer group of enterprises.” The Kiyoto *et al.* patent makes no mention of industry standards nor of peer groups, and it does not judge whether any computers have adequate security.

Claim 3 requires the peer group information to be “information derived from information previously obtained through application of the collecting and analyzing steps to two or more enterprises in the relevant peer group.” In other words, one audits several enterprises in the relevant peer group, combines the results to form an industry average or normal level of security, and then compares this industry average or normal level to the results obtained from auditing another individual enterprise. The Kiyoto *et al.* patent does not teach anything like this.

Claims 4, 14, 18, and 23 all require the generation of a report, such as that illustrated in Figure 6, which presents the results of a single enterprise audit and a peer group audit “in a way that facilitates their comparison” – for example, as illustrated in Figure 6. The Kiyoto *et al.* patent does not teach this.

Claim 5 calls for the audit results to be “broken down into several results relating to several different areas of security,” as is illustrated in Figure 6. The Kiyoto *et al.* patent does not teach including such a breakdown in a report.

Claims 6 and 8 require inclusion in the report both “physical security information” and “personnel security information” some of which information must be gathered using interviews, such as those illustrated in Figure 7 and in Appendix A. The Kiyoto *et al.* patent does not teach gathering security information using interviews.

Claim 7 requires inclusion in the report of both password security information and file access security information. The Kiyoto *et al.* patent does not teach how to audit password security or file access security. (These are taught in Figures 3 and 5 of the present application and in the accompanying text.)

Claim 9, like claim 6, calls specifically for the analysis of “node configuration security information” as well as “security information gathered through the use of interviews.” Claim 10 then adds to this analysis of “password security information” as taught, for example, in Figure 3. Claim 11 contribute to this analysis of “file access permission security information” as taught, for example, in Figure 5. The Kiyoto *et al.* patent does not teach any of these four topics.

Claim 12 requires the generation of two differently-formulated reports, one “for technical experts” and another “for non-technical-experts”. The Kiyoto *et al.* patent does not teach generating multiple reports directed to differing audiences.

Claims 13, 19, and 23 all add the requirement that commands be generated “to alter the security information of one or more nodes to improve system security in at least some cases when the analysis or comparison or both indicate security is in need of improvement,” as is illustrated in steps 322, 324, and 326 of Figure 3 and in steps 534 and 326 in Figure 5 and in the accompanying text, for example. The Kiyoto *et al.* patent does not teach altering configuration to improve security.

Claims 15 and 20 require the generation of commands “which force the deactivation or correction of one or more passwords” as is illustrated in steps 322, 324, and 326 of Figure 3 and in the accompanying text. The Kiyoto *et al.* patent does not teach automatic password deactivation or correction.

Claims 16 and 21 require the generation of commands “which force the alteration of one or more configuration file or control file access permissions” as is illustrated in steps 534 and 326 in Figure 5 and in the accompanying text. The Kiyoto *et al.* patent does not teach altering file access permissions automatically.

Accordingly, all of the dependant claims are in condition to be allowed.

E. Conclusion

Applicants believe that the present application, as amended, is now in condition for allowance. Early and favorable reconsideration and allowance of this application, as amended, is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

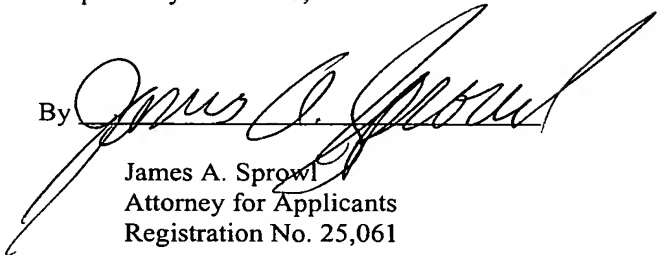
The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 08-2025. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 08-2025. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicants hereby petition for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 08-2025.

Respectfully submitted,

Date Feb. 7, 2007

FOLEY & LARDNER LLP
321 North Clark Street, Suite 2800
Chicago, Illinois 60610

Telephone: (312) 832-4586
Facsimile: (312) 832-4700

By 

James A. Sprowl
Attorney for Applicants
Registration No. 25,061

Telephone 847-446-7399